

#5
11-13-02
8/11

JC879 U.S. PTO
10/046224
01/16/02

500.41092X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): NISHIOKA, et al.
Serial No.: Not yet assigned
Filed: January 16, 2002
Title: PUBLIC-KEY CRYPTOGRAPHIC SCHEMES SECURE AGAINST
AN ADAPTIVE CHOSEN CIPHERTEXT ATTACK IN THE
STANDARD MODEL
Group: Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

January 16, 2002

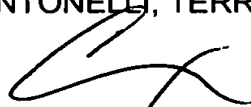
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby
claim(s) the right of priority based on Japanese Patent Application No.(s) 2001-009646,
filed January 18, 2001.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/alb
Attachment
(703) 312-6600

日本国特許庁
JAPAN PATENT OFFICE

#5
11-13
JC679 U.S. PTO
10/046224
01/16/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日
Date of Application:

2001年 1月18日

出願番号
Application Number:

特願2001-009646

出願人
Applicant(s):

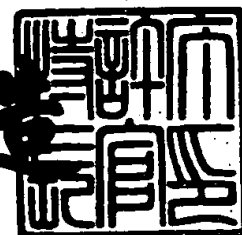
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年12月21日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 K00019191A

【提出日】 平成13年 1月18日

【あて先】 特許庁長官

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 西岡 玄次

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 佐藤 尚宜

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 瀬戸 洋一

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】	図面	1
【物件名】	要約書	1
【ブルーフの要否】	要	

【書類名】 明細書

【発明の名称】

標準モデル上で適応的選択暗号文攻撃に対して安全な公開鍵暗号方法

【特許請求の範囲】

【請求項1】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数1】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数2】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G' : 1 \text{ 対 } 1 \text{ 写像}$
- $\pi^{-1} : \text{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

なる公開鍵を作成し (但し、群 G は群 G' 部分群とし、 X_1, X_2 は正整数からなる有限集合で、

【数3】

$$\alpha_1 \parallel \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

を満たすものとする。また、 M は平文空間とする),

(1) 送信者は、平文 m ($m \in M$) に対して、乱数

$\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ を選び、

【数 4】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, m)h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{mr}$$

計算し (但し, $\alpha = \alpha_1 || \alpha_2$), (u_1, u_2, e, v) を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数 5】

$$\pi(\alpha'_1, \alpha'_2, m') = e/u_1^z$$

0 なる α'_1, α'_2, m' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, m' \in M$) を計算し、

【数 6】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_{11} + m' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + m' y_{22}} = v$$

が成立すれば復号化結果を m' とし (但し, $\alpha' = \alpha'_1 || \alpha'_2$), 成立しなければ該暗号文を拒否する旨を復号化結果として出力する

ことを特徴とする公開鍵暗号方法。

【請求項 2】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 7】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数 8】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)

なる公開鍵を作成し、

(1) 送信者は、平文 m ($|m|=k_3$, 但し $|x|$ は x の桁数を表す) に対して、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1|=k_1, |\alpha_2|=k_2$) を作成し、

【数 9】

$$M = \alpha || m$$

を計算し、さらに乱数 $r \in \mathbb{Z}_q$ を選び、

【数 10】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = M h^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{mr} \bmod p$$

計算し、 (u_1, u_2, e, v) を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数 1 1】

$$\alpha'_1 || \alpha'_2 || m' = e/u_1^z \bmod p$$

なる α'_1, α'_2, m' ($|\alpha'_1|=k_1, |\alpha'_2|=k_2, |m'|=k_3$) を計算し,

【数 1 2】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_{11} + m' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + m' y_{22}} \equiv v \pmod{p}$$

が成立すれば復号化結果を m' とし (但し, $\alpha' = \alpha'_1 || \alpha'_2$), 成立しなければ該暗号文を拒否する旨を復号化結果として出力することを特徴とする公開鍵暗号方法。

【請求項 3】

請求項 1 または 2 において, 前記公開情報は, 前記受信者が生成し, 公開するステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項 4】

請求項 1 において, 該送信者は該暗号文を作成するに当たり, 予め乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ を選び,

【数 1 3】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad h^r, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2}$$

を前もって計算して保存しておく

ことを特徴とする公開鍵暗号方法。

【請求項 5】

請求項 2 において, 該送信者は該暗号文を作成するに当たり, 予め乱数

α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in Z_q$ を選び,

【数 1 4】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad h^r \bmod p, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2} \bmod p$$

を前もって計算して保存しておく
ことを特徴とする公開鍵暗号方法。

【請求項 6】

送信者は、受信者に対して暗号化されたデータを送信する暗号通信方法であって

鍵生成のステップとして、

【数 1 5】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数 1 6】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}, d_1 = g_1^{y_{11}} g_2^{y_{12}}, d_2 = g_1^{y_{21}} g_2^{y_{22}}, h = g_1^z,$
- $\pi : X_1 \times X_2 \times M \longrightarrow G' : 1 \text{ 対 } 1 \text{ 写像}$
- $\pi^{-1} : \text{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : 対称型暗号化関数

なる公開鍵を作成し (但し、群 G は群 G' の部分群とし、 X_1, X_2 は正整数からなる有限集合で、

【数 17】

$$\alpha_1 || \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

を満たすものとする。また、 M は鍵空間とする、

(1) 送信者は鍵データ K ($K \in M$) に対して、乱数

$\alpha_1 \in X_1, \alpha_2 \in X_2, r \in \mathbb{Z}_q$ を選び、

【数 18】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{Kr}$$

計算し (但し、 $\alpha = \alpha_1 || \alpha_2$)、さらに、送信者は、送信データ m の暗号文 C を (対称型) 暗号化関数 E と鍵データ K を用いて、

【数 19】

$$C = E_K(m)$$

にて作成し、(u_1, u_2, e, v, C)を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数 20】

$$\pi(\alpha'_1 || \alpha'_2 || K') = e/u_1^z$$

なる α'_1, α'_2, K' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, K' \in M$) を計算し、

【数 2 1】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} = v$$

が成立すれば (但し, $\alpha' = \alpha'_1 || \alpha'_2$),

【数 2 2】

$$m = D_{K'}(C)$$

にて復号化を行い, 復号化結果を出力し, 成立しなければ該暗号文を拒否する旨
を復号化結果として出力する
ことを特徴とする暗号通信方法。

【請求項 7】

請求項 6 において, 該送信者は, 暗号文 C を (対称型) 暗号化関数 E と鍵データ K
, および公開された適当な関数 f を用いて,

【数 2 3】

$$C = E_K(f(\alpha_1, \alpha_2) || m)$$

にて作成し, 該受信者は,

【数 2 4】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} = v,$$

$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

が成立することを検査し (但し, f は k ビットの値を出力するものとし, $[x]^k$ は x
の上位 k ビットを表す), 検査をパスした場合に

【数25】

$$m = [D_{K'}(C)]^{-k}$$

により復号化を行う（但し、 $[x]^{-k}$ は x の上位 k ビットを除いたビット列を表す）

ことを特徴とする公開鍵暗号方法。

【請求項8】

送信者は、受信者に対して暗号化されたデータを送信する暗号通信方法であって

鍵生成のステップとして、

【数26】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数27】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)
- E : 対称型暗号化関数

なる公開鍵を作成し、

送信者は鍵データ K ($|K|=k_3$, 但し $|x|$ は x の桁数を表す) に対して、乱数

$\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1|=k_1, |\alpha_2|=k_2$) を作成し、

【数 28】

$$M = \alpha || K$$

を計算し、さらに乱数 $r \in \mathbb{Z}_q$ を選び、

【数 29】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = Mh^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{Kr} \bmod p$$

を計算し、さらに、送信者は、送信データ m の暗号文 C を（対称型）暗号化関数 E と鍵データ K を用いて、

【数 30】

$$C = E_K(m)$$

にて作成し、 (u_1, u_2, e, v, C) を暗号文として前記受信者に送信し、

前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数 31】

$$\alpha'_1 || \alpha'_2 || K' = e / u_1^z \bmod p$$

なる α'_1, α'_2, K' ($|\alpha'_1| = k_1, |\alpha'_2| = k_2, |K'| = k_3$) を計算し、

【数 32】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_{11} + K' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + K' y_{22}} \equiv v \pmod{p}$$

が成立すれば（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ）,

【数 3 3】

$$m = D_{K'}(C)$$

にて復号化を行い、復号化結果を出力し、成立しなければ該暗号文を拒否する旨
を復号化結果として出力する
ことを特徴とする暗号通信方法。

【請求項 9】

請求項 8 において、該送信者は、暗号文 C を（対称型）暗号化関数 E と鍵データ K
、および公開された適当な関数 f を用いて、

【数 3 4】

$$C = E_K(f(\alpha_1, \alpha_2) || m)$$

にて作成し、該受信者は、

【数 3 5】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} \equiv v \pmod{p},$$

$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

が成立することを検査し（但し、 f は k ビットの値を出力するものとし、 $[x]^k$ は x
の上位 k ビットを表す）、検査をパスした場合に

【数 3 6】

$$m = [D_{K'}(C)]^{-k}$$

により復号化を行う（但し、 $[x]^{-k}$ は x の上位 k ビットを除いたビット列を表す
）

ことを特徴とする公開鍵暗号方法。

【請求項10】

請求項6から請求項9のいずれかにおいて、前記公開情報は、前記受信者が生成し、公開するステップを備えることを特徴とする公開鍵暗号方法。

【請求項11】

請求項6または7において、該送信者は該暗号文を作成するに当たり、予め乱数 α_1, α_2 ($\alpha_1 \in X_1, \alpha_2 \in X_2$), $r \in \mathbb{Z}_q$ を選び、
【数37】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad h^r, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2}$$

を前もって計算して保存しておくことを特徴とする公開鍵暗号方法。

【請求項12】

請求項8または9において、該送信者は該暗号文を作成するに当たり、予め乱数 α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in \mathbb{Z}_q$ を選び、
【数38】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad h^r \bmod p, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2} \bmod p$$

を前もって計算して保存しておくことを特徴とする公開鍵暗号方法。

【請求項13】

送信者は、受信者に対して暗号化されたデータを送信する暗号通信方法であって、
鍵生成のステップとして、

【数39】

$$\bullet \quad x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数 4 0】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, $h = g_1^z$,
- $\pi : X_1 \times X_2 \times M \rightarrow \text{Dom}(E) : 1 \text{ 対 } 1 \text{ 写像}$ ($\text{Dom}(E)$ は関数 E の定義域)
- $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$
- H : ハッシュ関数
- E : 対称型暗号化関数

なる公開鍵を作成し (但し、群 G は群 G' の部分群とし、

X_1, X_2 は正整数からなる有限集合で、

【数 4 1】

$$\alpha_1 || \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

を満たすものとする) ,

(1) 送信者は、乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ を選び、

【数 4 2】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2}, \quad K = H(h^r)$$

計算し (但し、 $\alpha = \alpha_1 || \alpha_2$) , さらに、送信者は、送信データ m の暗号文 C を (対称型) 暗号化関数 E を用いて、

【数 4 3】

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

にて作成し、 (u_1, u_2, v, C) を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、

【数44】

$$K' = H(u_1^z)$$

を計算し、さらに該暗号文から、

【数45】

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

なる α'_1, α'_2 ($\alpha'_1 \in X_1, \alpha'_2 \in X_2$) を計算し、

【数46】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_1} u_2^{x_2 + \alpha'_1 y_2} = v,$$

が成立すれば（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ）， m' を復号化結果として出力し、成立しなければ該暗号文を拒否する旨を復号化結果として出力することとを特徴とする暗号通信方法。

【請求項14】

送信者は、受信者に対して暗号化されたデータを送信する暗号通信方法であって

鍵生成のステップとして、

【数47】

$$\bullet x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$$

なる秘密鍵を作成し、さらに、

【数 4 8】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)
- H : ハッシュ関数
- E : 対称型暗号化関数 (E の定義域は正整数全体とする)

なる公開鍵を作成し,

(1) 送信者は, 乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1, |\alpha_2| = k_2$, 但し $|x|$ は x の桁数を表す) を作成し, さらに乱数 $r \in \mathbb{Z}_q$ を選び,

【数 4 9】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2} \bmod p, \quad K = H(h^r \bmod p)$$

を計算し, さらに, 送信者は, 送信データ m の暗号文 C を (対称型) 暗号化関数を用いて,

【数 5 0】

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

にて作成し, (u_1, u_2, v, C) を暗号文として前記受信者に送信し,

(2) 前記受信者は, 自身の該秘密鍵を用いて,

【数 5 1】

$$K' = H(u_1^z \bmod p)$$

を計算し, さらに該暗号文から,

【数 5 2】

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

なる α'_1, α'_2 ($|\alpha'_1|=k_1, |\alpha'_2|=k_2$) を計算し,

【数 5 3】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 u_2 x_2} \equiv v \pmod{p}$$

が成立すれば (但し, $\alpha' = \alpha'_1 || \alpha'_2$), m' を復号化結果として出力し, 成立しなければ該暗号文を拒否する旨を復号化結果として出力する (ことを特徴とする暗号通信方法。

【請求項 1 5】

請求項 1 3 または 1 4 において, 前記公開情報は, 前記受信者が生成し, 公開するステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項 1 6】

請求項 1 3 において, 該送信者は該暗号文を作成するに当たり, 予め乱数 α_1, α_2 ($\alpha_1 \in X_1, \alpha_2 \in X_2$), $r \in \mathbb{Z}_q$ を選び, u_1, u_2, e, v を前もって計算して保存しておく

ことを特徴とする公開鍵暗号方法。

【請求項 1 7】

請求項 1 4 において, 該送信者は該暗号文を作成するに当たり, 予め乱数 α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in \mathbb{Z}_q$ を選び, u_1, u_2, e, v を前もって計算して保存しておく

ことを特徴とする公開鍵暗号方法。

【請求項 1 8】

送信者は, 受信者に対して暗号化されたデータを送信する暗号通信方法であって

鍵生成のステップとして、

【数 5 4】

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (非対称型暗号) 復号化鍵

なる秘密鍵を作成し、さらに、

【数 5 5】

- G : 有限 (乗法) 群
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2},$
- $\pi : X_1 \times X_2 \times M \rightarrow \text{Dom}(E) : 1 \text{ 対 } 1 \text{ 写像 (Dom}(E) \text{ は関数 } E \text{ の定義域)}$
- $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$
- $E_{pk}(\cdot) : (\text{非対称型暗号}) \text{ 暗号化関数}$

なる公開鍵を作成し (但し、群 G は群 G' の部分群とし、

X_1, X_2 は正整数からなる有限集合で、

【数 5 6】

$$\alpha_1 || \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

を満たすものとする。 M は平文空間) ,

(1) 送信者は、乱数 $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in \mathbb{Z}_q$ を選び、

【数 5 7】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2}$$

計算し (但し、 $\alpha = \alpha_1 || \alpha_2$) , さらに、送信者は、送信データ m の暗号文 C を (非対称型) 暗号化関数 E_{pk} を用いて、

【数58】

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

にて作成し、 (u_1, u_2, e, v) を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数59】

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

なる α'_1, α'_2, m' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, m' \in M$)を計算し、

【数60】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 u_2 x_2 + \alpha' y_2} = v$$

が成立すれば(但し、

【数61】

$$\alpha' = \alpha'_1 || \alpha'_2$$

とする) m' を復号化結果として出力し、成立しなければ該暗号文を拒否する旨を復号化結果として出力する

ことを特徴とする暗号通信方法。

【請求項19】

送信者は、受信者に対して暗号化されたデータを送信する暗号通信方法であって

鍵生成のステップとして、

【数62】

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (非対称型暗号) 復号化鍵

なる秘密鍵を作成し、さらに、

【数63】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$,
- k_1, k_2 : 正定数 ($10^{k_1+k_2} < q$)
- $E_{pk}(\cdot)$: (非対称型暗号) 暗号化関数 (定義域は正整数全体とする)

なる公開鍵を作成し、

(1) 送信者は、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1, |\alpha_2| = k_2$, 但し $|x|$ は x の桁数を表す) を作成し、さらに乱数 $r \in \mathbb{Z}_q$ を選び、

【数64】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2} \bmod p$$

を計算し、さらに、送信者は、送信データ m (正整数) の暗号文 C を (非対称型) 暗号化関数 E_{pk} を用いて、

【数65】

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

にて作成し、 (u_1, u_2, e, v) を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の該秘密鍵を用いて、該暗号文から、

【数 6 6】

$$\alpha'_1 || \alpha'_2 || m = D_{sk}(e)$$

なる α'_1, α'_2, m' ($|\alpha'_1|=k_1, |\alpha'_2|=k_2, m'$ は正整数) を計算し,

【数 6 7】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 u_2 x_2 + \alpha'_2 y_2} \equiv v \pmod{p},$$

が成立すれば (但し,

【数 6 8】

$$\alpha' = \alpha_1 || \alpha'_2$$

とする), m' を復号化結果として出力し, 成立しなければ該暗号文を拒否する旨を復号化結果として出力することを特徴とする暗号通信方法。

【請求項 20】

請求項 18 または 19 において, 前記公開情報は, 前記受信者が生成し, 公開するステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項 21】

請求項 18 において, 該送信者は該暗号文を作成するに当たり, 予め乱数 α_1, α_2 ($\alpha_1 \in X_1, \alpha_2 \in X_2$), $r \in Z_q$ を選び, u_1, u_2, v を前もって計算して保存しておく

ことを特徴とする公開鍵暗号方法。

【請求項 22】

請求項 19 において, 該送信者は該暗号文を作成するに当たり, 予め乱数 α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in Z_q$ を選び, u_1, u_2, v を前もって計算して保存し

ておく

ことを特徴とする公開鍵暗号方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、公開鍵暗号方法及び公開鍵暗号を用いた暗号通信に関する。

【 0 0 0 2 】

【従来の技術】

現在まで、様々な公開鍵暗号方式が提案されている。なかでも、
文献1「R. L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1978.」

に掲載されている方法が最も有名であり、最も実用化されている公開鍵暗号である。その他には、

文献2「V. S. Miller: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS218, Springer-Verlag, pp.417-426 (1985)」,

文献3「N. Koblitz: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, p.203-209 (1987)」

等に記載の楕円曲線を用いた方法が効率的な公開鍵暗号として知られている。

【 0 0 0 3 】

安全性について証明可能な方法として、まず、選択平文攻撃を対象としたものは、

文献4「M. O. Rabin: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」

に記載されている暗号方法、

文献5「T. ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, p.469-472(1985)」

に記載されている暗号方法,

文献6「S. Goldwasser and S. Micali: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984)」に記載されている暗号方法,

文献7「M. Blum and S. Goldwasser: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS196, Springer-Verlag, pp.289-299 (1985)」

に記載されている暗号方法,

文献8「S. Goldwasser and M. Bellare: Lecture Notes on Cryptography, <http://www-cse.ucsd.edu/users/mihir/> (1997)」

に記載されている暗号方法,

文献9「T. Okamoto and S. Uchiyama. A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS1403, Springer Verlag, pp.308-318 (1998)」

に記載されている暗号方法,

などが知られている。

【 0 0 0 4 】

また, 選択暗号文攻撃に対して安全性証明可能な方法としては,

文献10「D. Dolev, C. Dwork and M. Naor.: Non-malleable cryptography, In 23rd Annual ACM Symposium on Theory of Computing, pp.542-552 (1991)」

に記載されている暗号方法,

文献11「M. Naor and M. Yung.: Public-key cryptosystems provably secure against chosen ciphertext attacks, Proc. of STOC, ACM Press, pp.427-437 (1990)」

に記載されている暗号方法,

文献12「M. Bellare and P. Rogaway,. Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS950, Springer Verlag, pp.92-111 (1994)」

に記載されている暗号方法,

文献13「R. Cramer and V. Shoup: A Practical Public Key Cryptosystem Prov

ably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS1462, Springer-Verlag, pp.13-25 (1998)』

に記載されている暗号方法、などが知られている。また、

文献14「M. Bellare, A. Desai, D. Pointcheval and P. Rogaway. : Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS1462, Springer Verlag, pp.26-45 (1998)」

では、IND-CCA2（適応的選択暗号文攻撃に対して“強秘匿”であること）とNM-CA2（適応的選択暗号文攻撃に対して“頑強”であること）の等価性が示され、現在、この条件を満たす公開鍵暗号が最も安全であると考えられている。

【 0 0 0 5 】

【発明が解決しようとする課題】

文献12に記載されている公開鍵暗号方法は、実用的ではあるが、理想的ランダム関数の存在を前提として安全性の証明が行われている。理想的ランダム関数を実システムにおいて構築することは不可能なため、文献12の方法を実システムに適用する場合には、理想的ランダム関数の部分は実用的ハッシュ関数に置き換えられる。このため、実システムでは安全性の証明ができない。

【 0 0 0 6 】

文献13では、理想的ランダム関数の代わりに汎用一方向性ハッシュ関数の存在を前提としてIND-CCA2であることが証明できる公開鍵暗号方法を提供している。汎用一方向性ハッシュ関数は（暗号学的仮定の下で）実際に構築可能なので、文献13に記載されている方法は標準モデル上で安全性が証明できる方法である。しかし、実システムに適用する場合、効率性を高める目的で、SHA-1などの実用的なハッシュ関数を汎用的ハッシュ関数と仮定して用いるため、安全性証明可能な条件に強い仮定が必要になる。また、文献13では、汎用的一方向性ハッシュ関数の存在を前提としない公開鍵暗号方法も提案されているが、汎用的一方向性ハッシュ関数の存在を前提とする方法に比べて効率性が悪くなる。

【 0 0 0 7 】

本発明の主たる目的は、標準モデル（理想的関数の存在等を仮定しない現実の計算機モデル）で、最も強力な攻撃方法である適応的選択暗号文攻撃に対して安

全性の証明が可能であり (IND-CCA2), かつ, 実用的な公開鍵暗号方法を提供することである。

【0008】

本発明の他の目的は, Diffie-Hellman 決定問題の困難性のみを仮定し, 実システムに適用した場合においても, 安全性の証明が可能な実用的公開鍵暗号方法を提供することである。

【0009】

また, 本発明の他の目的は, 本発明に依る公開鍵暗号方法を用いた暗号通信方法, さらに, これらの方法を実行するプログラム, 装置またはシステムを提供することである。

【0010】

【課題を解決するための手段】

上記目的を達成するための手段として, 適応的選択暗号文攻撃に対しての安全性を確保するため, 不正な暗号文が (シミュレートされた) 復号化オラクルに入力された場合には拒否されるように, 平文と乱数を組み合わせて暗号文を作成する。復号化オラクルが与えられた環境とは, ターゲットとなる暗号文以外の任意の暗号文に対して, その復号化結果を無条件に得られる環境を指す。具体的な実現方法の1つとしては,

[鍵生成]

【0011】

【数69】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

【0012】

なる秘密鍵を作成し, さらに,

【0013】

【数 7 0】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)

【0 0 1 4】

なる公開鍵を作成する。

[暗号化]

送信者は、平文 m ($|m|=k_3$, 但し $|x|$ は x の桁数を表す) に対して、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1|=k_1, |\alpha_2|=k_2$) を作成し、

【0 0 1 5】

【数 7 1】

$$M = \alpha || m$$

【0 0 1 6】

を計算する。さらに、乱数 $r \in \mathbb{Z}_q$ を選び、

【0 0 1 7】

【数 7 2】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = M h^r \bmod p, \quad v = g_1^{\alpha_1 c^r} d_1^{\alpha r} d_2^{mr} \bmod p$$

【0 0 1 8】

を計算し、 (u_1, u_2, e, v) を暗号文として前記受信者に送信する。

[復号化]

受信者は、自身の秘密鍵を用いて、暗号文から、

【0 0 1 9】

【数 7 3】

$$\alpha'_1 || \alpha'_2 || m' = e/u_1^z \bmod p$$

【0020】

なる α'_1, α'_2, m' ($|\alpha'_1|=k_1, |\alpha'_2|=k_2, |m'|=k_3$) を計算し,

【0021】

【数 7 4】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_{11} + m' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + m' y_{22}} \equiv v \pmod{p}$$

【0022】

が成立すれば m' を復号化結果として出力し (但し, $\alpha' = \alpha'_1 || \alpha'_2$), 成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0023】

【発明の実施の形態】

暗号化装置, 復号化装置が新規, 図4が無い, 図が少ない

以下, 図面を用いて, 本発明の実施例について説明する。

【0024】

図1は, 本発明の実施例のシステム構成を示す図である。このシステムは, 送信者側装置100と受信者側装置200から構成されている。さらに, 送信者側装置100と受信者側装置200は通信回線300で接続されている。

【0025】

図2は, 実施例における送信者側装置100の内部構成を示す。送信者側装置100は, 乱数生成手段101, べき乗算手段102, 演算手段103, 剰余演算手段104, メモリ105, 通信装置106, 入力装置107, 暗号化装置108を備えている。暗号化対象となる平文 m は, 入力装置107を用いて入力するか, 送信者側装置100上で作成するか, または, 通信装置106あるいは図示していない記憶媒体を介して取り込む。

【0026】

図3は, 実施例における受信者側装置200の内部構成を示す。受信者側装置200

は、鍵生成手段201、べき乗算手段202、剰余演算手段203、演算手段204、メモリ205、通信装置206、復号化装置108、を備えている。このほか、図示していないが、復号化結果を、表示、音などの手段により当該装置の使用者（受信者）に示すための出力装置を備える。

【 0 0 2 7 】

送信者側装置100、受信者側装置200は、いずれもCPUとメモリとを備えた計算機を用いて所定のプログラムを実行させることにより構成することができる。乱数生成手段101、鍵生成手段201、べき乗算手段202、剰余演算手段203はいずれも専用のハードウェアを用いて構成しても良いし、演算手段上(CPU)上で動作するプログラムとして構成しても良い。各プログラムは、可搬型記憶媒体や通信回線上の通信媒体といった計算機が読みとり可能な媒体上に具現化され、これらの媒体を介して計算機のメモリに格納される。

【 0 0 2 8 】

図4は、実施例2の概要を示す図である。

【 0 0 2 9 】

図5は、実施例4の概要を示す図である。

【 0 0 3 0 】

図6は、実施例6の概要を示す図である。

(実施例1)

本実施例は、公開鍵暗号方法について説明する。

【 0 0 3 1 】

図1は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【 0 0 3 2 】

【数75】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

【0033】

なる秘密情報を作成し、

【0034】

【数76】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G' : 1$ 対 1 写像
- $\pi^{-1} : \text{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

【0035】

なる公開情報を作成し (但し, 群 G は群 G' の部分群とし, X_1, X_2 は正整数からなる有限集合で、

【0036】

【数77】

$$\alpha_1 \parallel \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

【0037】

を満たすものとする。また, M は平文空間とする), 公開情報を通信回線300などを介して出力し, 送信者側装置100へ送付するか, または公開する。公開する方法として, 例えば第3者 (公開情報管理機関) への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ205に格納する。

2. 暗復号化处理

(1) 送信者側装置100は, 送信者Aの操作により, 平文 m ($m \in M$) に対して, 乱数生成手段101を用いて, 乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ を選び, べき乗算手段102, 演算手段103, 剰余演算手段104を用いて,

【0038】

【数78】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, m)h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{mr}$$

【0039】

を計算する（但し、 $\alpha = \alpha_1 || \alpha_2$ ）。さらに、送信者側装置100は、送信者Aの操作により、 (u_1, u_2, e, v) を暗号文として、通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

（2）受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文から、

【0040】

【数79】

$$\pi(\alpha'_1, \alpha'_2, m') = e/u_1^z$$

【0041】

なる α'_1, α'_2, m' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, m' \in M$) を計算し、

【0042】

【数80】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha'_1 y_{11} + m' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + m' y_{22}} = v$$

【0043】

が成立すれば m' を復号化結果として出力し（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ），成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0044】

本実施例による方法では、GにおけるDiffie-Hellman 決定問題の困難性を前提として、適応的選択暗号文攻撃に対して強秘匿であることを示すことができる。

GにおけるDiffie-Hellman 決定問題とは、「 $g_1, g_2 \in G$ に対して、

【0045】

【数 8 1】

$$D = \{(g_1, g_2, g_1^r, g_2^r) \mid r \in \mathbb{Z}_q\}, \quad R = \{(g_1, g_2, g_1^{r_1}, g_2^{r_2}) \mid r_1, r_2 \in \mathbb{Z}_q, r_1 \neq r_2\}$$

【0046】

のいずれかの集合に属するシーケンス δ が与えられたとき、 δ がいずれに属するかを言い当てる問題」である。Diffie-Hellman 決定問題を $1/2$ よりも良い確率で解くことが難しいとき、Diffie-Hellman 決定問題は困難であると言う (Diffie-Hellman 決定問題については、文献13等に述べられている)。

安全性の証明方法の手順としては、本実施例の方法を破るアルゴリズムが存在すれば、そのアルゴリズムを利用して、(具体的には、文献12で述べられている方法と同様の方法にて)、Diffie-Hellman 決定問題を解くアルゴリズムを構築することができることを示す。

また、Diffie-Hellman 決定問題を解くアルゴリズムが存在したとしても、本実施例の方法を破るアルゴリズムは見つかっていないため、本実施例の方法を破る事は少なくともDiffie-Hellman 決定問題を解く以上に困難である。

【0047】

さらに、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ を選び、

【0048】

【数 8 2】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad h^r, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2}$$

【0049】

を前もって計算して保存しておくことが可能である。これにより、暗号化処理の負担を大幅に減らし処理時間を短縮することが可能になる。

(実施例2)

本実施例は、実施例1における公開鍵暗号方法の実現方法の1つについて述べる。

【0050】

図 1 は、本実施例のシステム構成を示す。図 4 は本実施例の概要を示す。

1. 鍵生成処理

受信者側装置 200 内の鍵生成手段 201 は、受信者 B の操作により、予め、

【 0 0 5 1 】

【 数 8 3 】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

【 0 0 5 2 】

なる秘密情報を作成し、

【 0 0 5 3 】

【 数 8 4 】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)

【 0 0 5 4 】

なる公開情報を作成し、公開情報を通信回線 300 などを介して出力し、送信者側装置 100 へ送付するか、または公開する。公開する方法として、例えば第 3 者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ 205 に格納する。

2. 暗復号化処理

(1) 送信者側装置 100 は、送信者 A の操作により、平文 m ($|m|=k_3$, 但し $|x|$ は x の桁数を表す) に対して、乱数生成手段 101 を用いて、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1|=k_1, |\alpha_2|=k_2$) を選び、

【 0 0 5 5 】

【数 85】

$$M = \alpha || m$$

【0056】

を計算し、さらに、乱数生成手段101を用いて、乱数 $r \in \mathbb{Z}_q$ を選び、べき乗算手段102、演算手段103、剰余演算手段104を用いて、

【0057】

【数 86】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = Mh^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{mr} \bmod p$$

【0058】

を計算する。さらに、送信者側装置100は、送信者Aの操作により、 (u_1, u_2, e, v) を暗号文として、通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0059】

(2) 受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文から、

【0060】

【数 87】

$$\alpha'_1 || \alpha'_2 || m' = e / u_1^z \bmod p$$

【0061】

なる α'_1, α'_2, m' ($|\alpha'_1| = k_1, |\alpha'_2| = k_2, |m'| = k_3$) を計算し、

【0062】

【数 88】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_1 y_{11} + m' y_{21}} u_2^{x_2 + \alpha'_1 y_{12} + m' y_{22}} \equiv v \pmod{p}$$

【0063】

が成立すれば m' を復号結果として出力し（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ），成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0064】

本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in \mathbb{Z}_q$ を選び、

【0065】

【数 89】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad h^r \bmod p, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2} \bmod p$$

【0066】

を前もって計算して保存しておくことで、暗号化処理負担を大幅に減少させることが可能である。

(実施例 3)

本実施例は、共通鍵暗号（対称型暗号）を用いて、メッセージの送信者であるAが受信者であるBに対して、送信データ m を暗号化し、暗号化鍵を実施例1で述べた公開鍵暗号により暗号化して鍵配送する場合について説明する。

【0067】

図1は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【0068】

【数90】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

【0069】

なる秘密情報を作成し、

【0070】

【数91】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G' : 1$ 対 1 写像
- $\pi^{-1} : \text{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : 対称型暗号化関数

【0071】

なる公開情報を作成し (但し、群 G は群 G' の部分群とし、 X_1, X_2 は正整数からなる有限集合で、

【0072】

【数92】

$$\alpha_1 \parallel \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

【0073】

を満たすものとする。また、 M は鍵空間とする)、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者 (公開情報管理機関) への登録など、周知の方法を用いる

ことが可能である。その他の情報については、メモリ205に格納する。

2. 暗復号化处理

(1) 送信者側装置100は、送信者Aの操作により、鍵データK ($K \in M$) に対して、乱数生成手段101を用いて、乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ を選び、べき乗算手段102, 演算手段103, 剰余演算手段104を用いて、

【0074】

【数93】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{Kr}$$

【0075】

を計算し (但し, $\alpha = \alpha_1 || \alpha_2$), 送信データmの暗号文Cを (対称型) 暗号化関数Eとその鍵データKを用いて、

【0076】

【数94】

$$C = E_K(m)$$

【0077】

にて作成する。さらに、送信者側装置100は、送信者Aの操作により、(u_1, u_2, e, v, C)を暗号文として、通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

(2) 受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202, 剰余演算手段203, 演算手段204を用いて暗号文から、

【0078】

【数95】

$$\pi(\alpha'_1 || \alpha'_2 || K') = e/u_1^z$$

【0079】

なる α'_1, α'_2, K' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, K' \in M$) を計算し,

【0080】

【数96】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} = v$$

【0081】

が成立すれば (但し, $\alpha' = \alpha'_1 || \alpha'_2$),

【0082】

【数97】

$$m = D_{K'}(C)$$

【0083】

にて復号化を行い、復号化結果を出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0084】

暗号文Cの別なる作成方法としては、該送信者は、暗号文Cを (対称型) 暗号化関数Eとその鍵データKを用いて、

【0085】

【数98】

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

【0086】

にて作成し、該受信者は、

【0087】

【数99】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} = v,$$

$$\alpha'_1 \parallel \alpha'_2 = [D_{K'}(C)]^{k_1 + k_2}$$

【0088】

が成立することを検査し（但し、 $[x]^k$ は x の上位 k 桁を表す。）、検査をパスした場合に

【0089】

【数100】

$$m = [D_{K'}(C)]^{-(k_1 + k_2)}$$

【0090】

により、復号化を行う。但し、 $[x]^{-k}$ は x の上位 k 桁を除いた整数列を表す。

【0091】

さらに、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ を選び、

【0092】

【数101】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad h^r, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2}$$

【0093】

を前もって計算して保存しておくことが可能である。これにより、暗号化処理の負担を大幅に減らし処理時間を短縮することが可能になる。

(実施例4)

本実施例は、共通鍵暗号（対称型暗号）を用いて、メッセージの送信者である

Aが受信者であるBに対して、送信データ m を暗号化し、暗号化鍵を実施例2で述べた公開鍵暗号により暗号化して鍵配送する場合について説明する。

【0094】

図1は、本実施例のシステム構成を示す。また、図5は、本実施例の概要を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【0095】

【数102】

$$\bullet x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

【0096】

なる秘密情報を作成し、

【0097】

【数103】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)
- E : 対称型暗号化関数

【0098】

なる公開情報を作成し、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

2. 暗復号化处理

(1) 送信者側装置100は、送信者Aの操作により、鍵データ K ($|K|=k_3$, 但し $|x|$ は x の桁数を表す。) に対して、乱数生成手段101を用いて、乱数 $\alpha = \alpha_1 || \alpha_2$

$(|\alpha_1|=k_1, |\alpha_2|=k_2)$ を選び,

【0099】

【数104】

$$M = \alpha || K$$

【0100】

を計算し、さらに、乱数生成手段101を用いて、乱数 $r \in \mathbb{Z}_q$ を選び、べき乗算手段102、演算手段103、剰余演算手段104を用いて、

【0101】

【数105】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = Mh^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{mr} \bmod p$$

【0102】

を計算する。さらに、送信者側装置100は、送信者Aの操作により、送信データ m の暗号文 C を（対称型）暗号化関数 E とその鍵データ K を用いて、

【0103】

【数106】

$$C = E_K(m)$$

【0104】

にて作成し、 (u_1, u_2, e, v, C) を暗号文として、通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

(2) 受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文から、

【0105】

【数107】

$$\alpha'_1 || \alpha'_2 || K' = e/u_1^z \bmod p$$

【0106】

なる α'_1, α'_2, K' ($|\alpha'_1|=k_1, |\alpha'_2|=k_2, |K'|=k_3$) を計算し,

【0107】

【数108】

$$g_1^{\alpha'_1 u_1^{x_1 + \alpha'_1 y_{11} + K' y_{21}}} u_2^{x_2 + \alpha'_1 y_{12} + K' y_{22}} \equiv v \pmod{p}$$

【0108】

が成立すれば (但し, $\alpha' = \alpha'_1 || \alpha'_2$),

【0109】

【数109】

$$m = D_{K'}(C)$$

【0110】

にて復号化を行い、復号化結果を出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0111】

暗号文Cの別なる作成方法としては、送信者は、暗号文Cを (対称型) 暗号化関数Eとその鍵データKを用いて、

【0112】

【数 110】

$$C = E_K(\alpha_1 || \alpha_2 || K)$$

【0113】

にて作成し、該受信者は、

【0114】

【数 111】

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha' y_{11} + K' y_{21}} u_2^{x_2 + \alpha' y_{12} + K' y_{22}} \equiv v \pmod{p},$$

$$\alpha'_1 || \alpha'_2 = [D_{K'}(C)]^{k_1 + k_2}$$

【0115】

が成立することを検査し、検査をパスした場合に

【0116】

【数 112】

$$m = [D_{K'}(C)]^{-(k_1 + k_2)}$$

【0117】

により復号化を行う。但し、 $[x]^{-k}$ は x の上位 k 桁を除いた整数列を表す。

【0118】

本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 α_1, α_2 ($|\alpha_1|=k_1, |\alpha_2|=k_2$), $r \in \mathbb{Z}_q$ を選び、

【0119】

【数 113】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad h^r \bmod p, \quad g_1^{\alpha_1} c^r d_1^{\alpha_2} \bmod p$$

【0120】

を前もって計算して保存しておくことで、暗号化処理負担を大幅に減少させるこ

とが可能である。

(実施例 5)

本実施例は、実施例 1 で述べた公開鍵暗号をベースに対称型暗号を用いて、メッセージの送信者である A が受信者である B に対して、送信データ m を暗号通信によって送信する場合について説明する。本実施例によれば、実施例 3 の方法に比べて効率性に優れ、対称型暗号が選択平文攻撃に対して頑強 (IND-CPA) であるとき、最強暗号 (NM-CCA2) であることが証明できる。また、本実施例による方式では、鍵 K 自身を送信するのではなく、各々が作成できるようにシードを共有させている。

【0 1 2 1】

図 1 は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者側装置 200 内の鍵生成手段 201 は、受信者 B の操作により、予め、

【0 1 2 2】

【数 1 1 4】

$$\bullet x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$$

【0 1 2 3】

なる秘密情報を作成し、

【0 1 2 4】

【数 1 1 5】

- G, G' : 有限 (乗法) 群, $G \subseteq G'$
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, h = g_1^z,$
- $\pi : X_1 \times X_2 \times M \longrightarrow \text{Dom}(E) : 1 \text{ 対 } 1 \text{ 写像 (Dom}(E) \text{ は関数 } E \text{ の定義域)}$
- $\pi^{-1} : \text{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- H : ハッシュ関数
- E : 対称型暗号化関数

【0 1 2 5】

なる公開情報を作成し (但し, 群 G は群 G' の部分群とし, X_1, X_2 は正整数からなる有限集合で,

【0 1 2 6】

【数 1 1 6】

$$\alpha_1 \parallel \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

【0 1 2 7】

を満たすものとする。), 公開情報を通信回線300などを介して出力し, 送信者側装置100へ送付するか, または公開する。公開する方法として, 例えば第3者 (公開情報管理機関) への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ205に格納する。

2. 暗復号化处理

(1) 送信者側装置100は, 送信者Aの操作により, 送信データ m ($m \in M$, M は平文空間) に対して, 乱数生成手段101を用いて, 乱数 $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in \mathbb{Z}_q$ を選び, べき乗算手段102, 演算手段103, 剰余演算手段104を用いて,

【0 1 2 8】

【数 1 1 7】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2}, \quad K = H(h^r)$$

【0129】

を計算し（但し， $\alpha = \alpha_1 || \alpha_2$ ），送信データ m の暗号文 C を（対称型）暗号化関数 E を用いて，

【0130】

【数118】

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

【0131】

にて作成する。さらに，送信者側装置100は，送信者Aの操作により， $(u_1, u_2, , v, C)$ を暗号文として，通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

（2）受信者側装置200は，受信者Bの操作により，保持している上記秘密情報と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて，

【0132】

【数119】

$$K' = H(u_1^z)$$

【0133】

を計算し，さらに暗号文から，

【0134】

【数120】

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

【0135】

なる α'_1, α'_2 ($\alpha'_1 \in X_1, \alpha'_2 \in X_2$) を計算し、

【0136】

【数121】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 y_1 u_2 x_2 + \alpha'_2 y_2} = v,$$

【0137】

が成立すれば（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ）,

m' を復号化結果を出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0138】

さらに、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in \mathbb{Z}_q$ を選び、 u_1, u_2, v を前もって計算して保存しておくことが可能である。これにより、暗号化処理の負担を大幅に減らし処理時間を短縮することが可能になる。

（実施例6）

本実施例は、実施例2で述べた公開鍵暗号をベースに対称型暗号を用いて、メッセージの送信者であるAが受信者であるBに対して、送信データ m を暗号通信によって送信する場合について説明する。

【0139】

図1は、本実施例のシステム構成を示す。また、図6は、本実施例の概要を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【0140】

【数122】

$$\bullet x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$$

【0141】

なる秘密情報を作成し、

【0142】

【数123】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$, $h = g_1^z \bmod p$,
- k_1, k_2, k_3 : 正定数 ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)
- H : ハッシュ関数
- E : 対称型暗号化関数 (E の定義域は正整数全体とする)

【0143】

なる公開情報を作成し、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

2. 暗復号化处理

送信者側装置100は、送信者Aの操作により、平文 m に対して、乱数生成手段101を用いて、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1, |\alpha_2| = k_2$, 但し $|x|$ は x の桁数を表す) を選び、さらに、乱数生成手段101を用いて、乱数 $r \in \mathbb{Z}_q$ を選び、べき乗算手段102、演算手段103、剰余演算手段104を用いて、

【0144】

【数124】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2} \bmod p, \quad K = H(h^r \bmod p)$$

【0145】

を計算する。さらに、送信者側装置100は、送信者Aの操作により、送信データ m の暗号文 C を（対称型）暗号化関数 E を用いて、

【0146】

【数 125】

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

【0147】

にて作成し、 (u_1, u_2, v, C) を暗号文として、通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

【0148】

受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて

【0149】

【数 126】

$$K' = H(u_1^z \bmod p)$$

【0150】

を計算し、さらに暗号文から、

【0151】

【数 127】

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

【0152】

なる α'_1, α'_2 ($|\alpha'_1| = k_1, |\alpha'_2| = k_2$) を計算し、

【0153】

【数 1 2 8】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 y_1 u_2 x_2 + \alpha'_2 y_2} \equiv v \pmod{p}$$

【0 1 5 4】

が成立すれば（但し、 $\alpha' = \alpha'_1 || \alpha'_2$ ），
 m' を復号化結果として出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。

【0 1 5 5】

さらに、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 $\alpha_1, \alpha_2 (|\alpha_1|=k_1, |\alpha_2|=k_2)$, $r \in \mathbb{Z}_q$ を選び、 u_1, u_2, v を前もって計算して保存しておくことが可能である。これにより、暗号化処理の負担を大幅に減らし処理時間を短縮することが可能になる。

（実施例 7）

本実施例は、実施例 1 で述べた公開鍵暗号と他の非対称型暗号を用いて、メッセージの送信者である A が受信者である B に対して、送信データ m を暗号通信によって送信する場合について説明する。本実施例によれば、他の弱い非対称型暗号（NM-CPA）を最強暗号（NM-CCA2）に変換することができる。

【0 1 5 6】

図 1 は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【0 1 5 7】

【数 1 2 9】

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : （非対称型暗号）復号化鍵

【0 1 5 8】

なる秘密情報を作成し、

【0159】

【数130】

- G : 有限 (乗法) 群
- q : 素数 (G の位数)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$,
- $\pi: X_1 \times X_2 \times M \rightarrow \text{Dom}(E)$: 1対1写像 ($\text{Dom}(E)$ は関数 E の定義域)
- $\pi^{-1}: \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$
- $E_{pk}(\cdot)$: (非対称型暗号) 暗号化関数

【0160】

なる公開情報を作成し (但し、群 G は群 G' の部分群とし、 X_1, X_2 は正整数からなる有限集合で、

【0161】

【数131】

$$\alpha_1 \parallel \alpha_2 < q \quad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

を満たすものとする。 M は平文空間) 、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者 (公開情報管理機関) への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

2. 暗復号化处理

(1) 送信者側装置100は、送信者Aの操作により、乱数生成手段101を用いて、乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ を選び、べき乗算手段102、演算手段103、剰余演算手段104を用いて、

【0162】

【数 132】

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2}$$

【0163】

を計算し（但し， $\alpha = \alpha_1 || \alpha_2$ ），送信データ m の暗号文 C を（非対称型）暗号化関数 E_{pk} を用いて，

【0164】

【数 133】

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

にて作成する。さらに，送信者側装置100は，送信者 A の操作により， (u_1, u_2, e, v) を暗号文として，通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

（2）受信者側装置200は，受信者 B の操作により，保持している上記秘密情報と，受信者側装置200内のべき乗算手段202，剰余演算手段203，演算手段204を用いて暗号文から，

【0165】

【数 134】

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

【0166】

なる α'_1, α'_2, m' ($\alpha'_1 \in X_1, \alpha'_2 \in X_2, m' \in M$) を計算し，

【0167】

【数 135】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_1 y_1 u_2 x_2 + \alpha'_1 y_2} = v$$

【0168】

が成立すれば（但し、

【0169】

【数 136】

$$\alpha' = \alpha'_1 || \alpha'_2$$

【0170】

とする) m' を復号化結果として出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。さらに、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ を選び、 u_1, u_2, v を前もって計算して保存しておくことが可能である。これにより、暗号化処理の負担を大幅に減らし処理時間を短縮することが可能になる。

(実施例 8)

本実施例は、実施例7と同様に、実施例2で述べた公開鍵暗号をベースに非対称型暗号を用いて、メッセージの送信者であるAが受信者であるBに対して、送信データ m を暗号通信によって送信する場合について説明する。

【0171】

図1は、本実施例のシステム構成を示す。また、図6は、本実施例の概要を示す。

1. 鍵生成処理

受信者側装置200内の鍵生成手段201は、受信者Bの操作により、予め、

【0172】

【数137】

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (非対称型暗号) 復号化鍵

【0173】

なる秘密情報を作成し、

【0174】

【数138】

- p, q : 素数 (q は $p-1$ の素因数) .
- $g_1, g_2 \in \mathbb{Z}_p$: $\text{ord}_p(g_1) = \text{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d = g_1^{y_1} g_2^{y_2} \bmod p$,
- k_1, k_2 : 正定数 ($10^{k_1+k_2} < q$)
- $E_{pk}(\cdot)$: (非対称型暗号) 暗号化関数 (定義域は正整数全体とする)

【0175】

なる公開情報を作成し、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

2. 暗復号化处理

送信者側装置100は、送信者Aの操作により、乱数生成手段101を用いて、乱数 $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1, |\alpha_2| = k_2$, 但し $|x|$ は x の桁数を表す) を選び、さらに、乱数生成手段101を用いて、乱数 $r \in \mathbb{Z}_q$ を選び、べき乗算手段102、演算手段103、剰余演算手段104を用いて、

【0176】

【数 139】

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha_2 r} \bmod p$$

【0177】

を計算する。さらに、送信者側装置100は、送信者Aの操作により、送信データm（正整数）の暗号文Cを（非対称型）暗号化関数Eを用いて、

【0178】

【数 140】

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

【0179】

にて作成し、 (u_1, u_2, e, v) を暗号文として、通信装置106を用いて通信回線300を介して受信者側装置200に送信する。

【0180】

受信者側装置200は、受信者Bの操作により、保持している上記秘密情報と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文から、

【0181】

【数 141】

$$\alpha'_1 || \alpha'_2 || m = D_{sk}(e)$$

【0182】

なる α'_1, α'_2, m' ($|\alpha'_1|=k_1, |\alpha'_2|=k_2, m'$ は正整数) を計算し、

【0183】

【数 142】

$$g_1^{\alpha'_1 u_1 x_1 + \alpha'_2 u_2 x_2 + \alpha'_3 v} \equiv v \pmod{p},$$

【0184】

が成立すれば（但し、

【0185】

【数 143】

$$\alpha' = \alpha_1 || \alpha'_2$$

【0186】

とする）、 m' を復号化結果として出力する。成立しなければ該暗号文を拒否する旨を復号化結果として出力する。また、本実施例による方法では、送信者側装置100は、送信者Aの操作により暗号文を作成するに当たり、予め乱数 α_1, α_2 （ $|\alpha_1|=k_1, |\alpha_2|=k_2$ ）、 $r \in \mathbb{Z}_q$ を選び、 u_1, u_2, v を前もって計算して保存しておくことで、暗号化処理負担を大幅に減少させることが可能である。

【0187】

以上、各実施例では、送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが、具体的には様々なシステムに適用される。

【0188】

例えば、電子ショッピングシステムでは、送信者はユーザであり、送信者側装置はパソコンなどの計算機であり、受信者は小売店またはその従業者、受信者側装置は小売店側装置、具体的には当該店舗におけるパソコンなどの計算機となる。このとき、ユーザが注文した商品等の注文書または注文書を暗号化した鍵は、本実施例による方法により暗号化されて小売店側装置に送信される。

【0189】

また、電子メール暗号化システムでは、各々の装置はパソコンなどの計算機であり、送信者のメッセージまたはメッセージを暗号化した鍵は、本実施例による

方法により暗号化されて受信者の計算機に送信される。

【 0 1 9 0 】

その他にも、従来の暗号化技術が使われている様々なシステムに適用することが可能である。

【 0 1 9 1 】

したがって、各実施例における平文 m またはメッセージ m には、さまざまなデジタル化されたデータ（マルチメディアデータ）を適用することができる。

【 0 1 9 2 】

なお、本実施例における各計算は、CPU がメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムだけではなく、いずれかがハードウェア化された演算装置であって、他の演算装置や、CPU と、データのやりとりを行うものであっても良い。

【 0 1 9 3 】

【発明の効果】

本発明の公開鍵暗号方法により、最も強力な攻撃法である適応的選択暗号文攻撃に対して安全であることが保証された効率的な暗号通信と、その応用装置、システムを実現することができる。

【図面の簡単な説明】

【図 1】

本発明の実施例のシステム構成を示す図である。

【図 2】

本発明の実施例における送信者側装置の内部構成を示す図である。

【図 3】

本発明の実施例における受信者側装置の内部構成を示す図である。

【図 4】

本発明の実施例 2 の概要を示す図である。

【図 5】

本発明の実施例 4 の概要を示す図である。

【図 6】

本発明の実施例 6 の概要を示す図である。

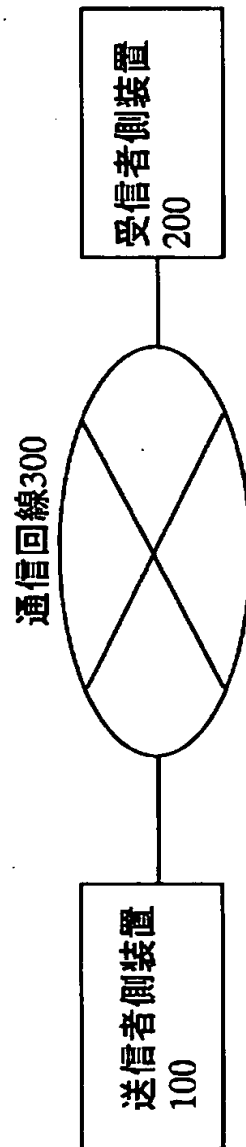
【符号の説明】

1 0 0 …送信者側装置, 1 0 1 …送信者側装置 1 0 0 内の乱数生成手段, 1 0 2 …送信者側装置 1 0 0 内のべき乗算手段, 1 0 3 …送信者側装置 1 0 0 内の演算手段, 1 0 4 …送信者側装置 1 0 0 内の剰余演算手段, 1 0 5 …送信者側装置 1 0 0 内のメモリ, 1 0 6 …送信者側装置 1 0 0 内の通信装置, 1 0 7 …送信者側装置 1 0 0 内の入力装置, 1 0 8 …送信者側装置 1 0 0 内の暗号化装置, 2 0 0 …受信者側装置, 2 0 1 …受信者側装置 2 0 0 内の鍵生成手段, 2 0 2 …受信者側装置 2 0 0 内のべき乗算手段, 2 0 3 …受信者側装置 2 0 0 内の剰余演算手段, 2 0 4 …受信者側装置 2 0 0 内の演算手段, 2 0 5 …受信者側装置 2 0 0 内のメモリ, 2 0 6 …受信者側装置 2 0 0 内の通信装置, 2 0 7 …受信者側装置 2 0 0 内の復号化装置, 3 0 0 …通信回線。

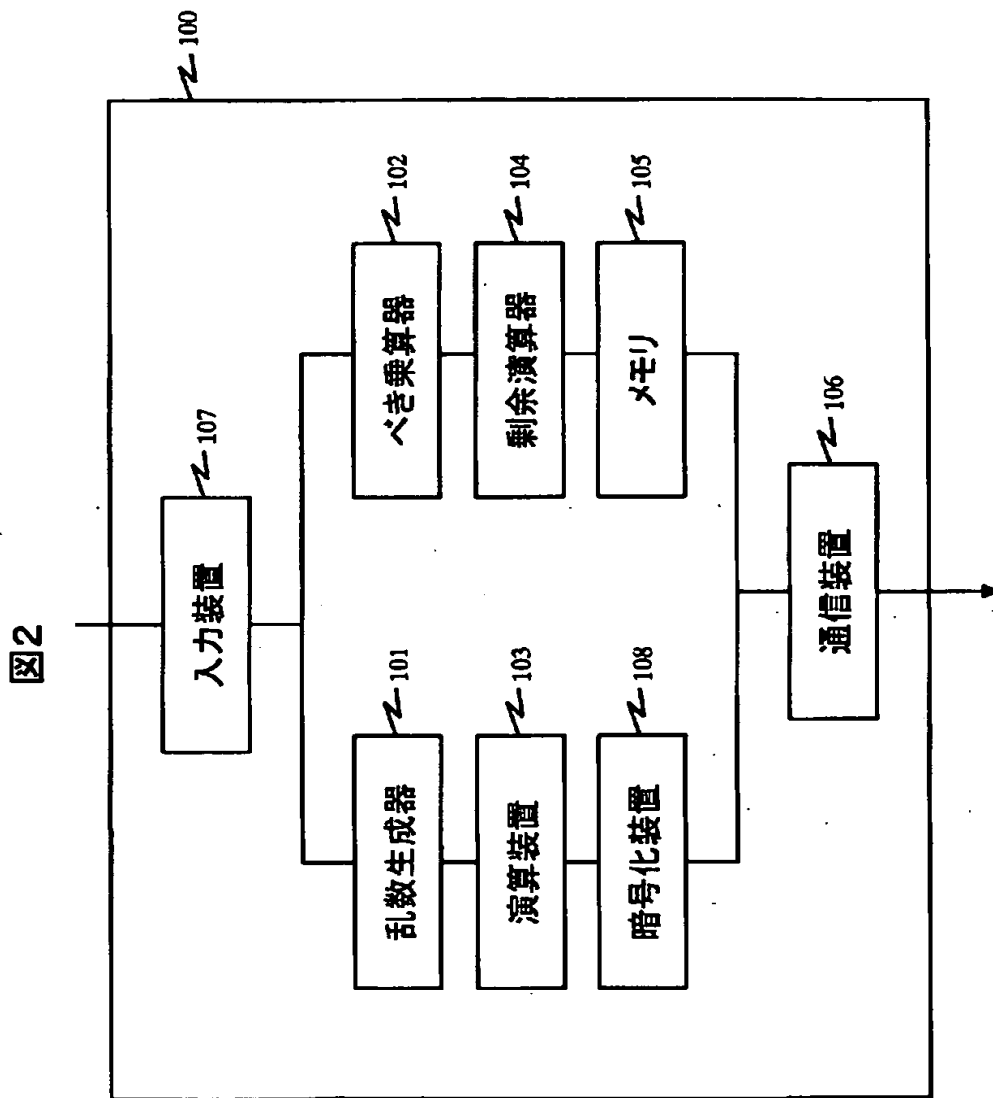
【書類名】 図面

【図1】

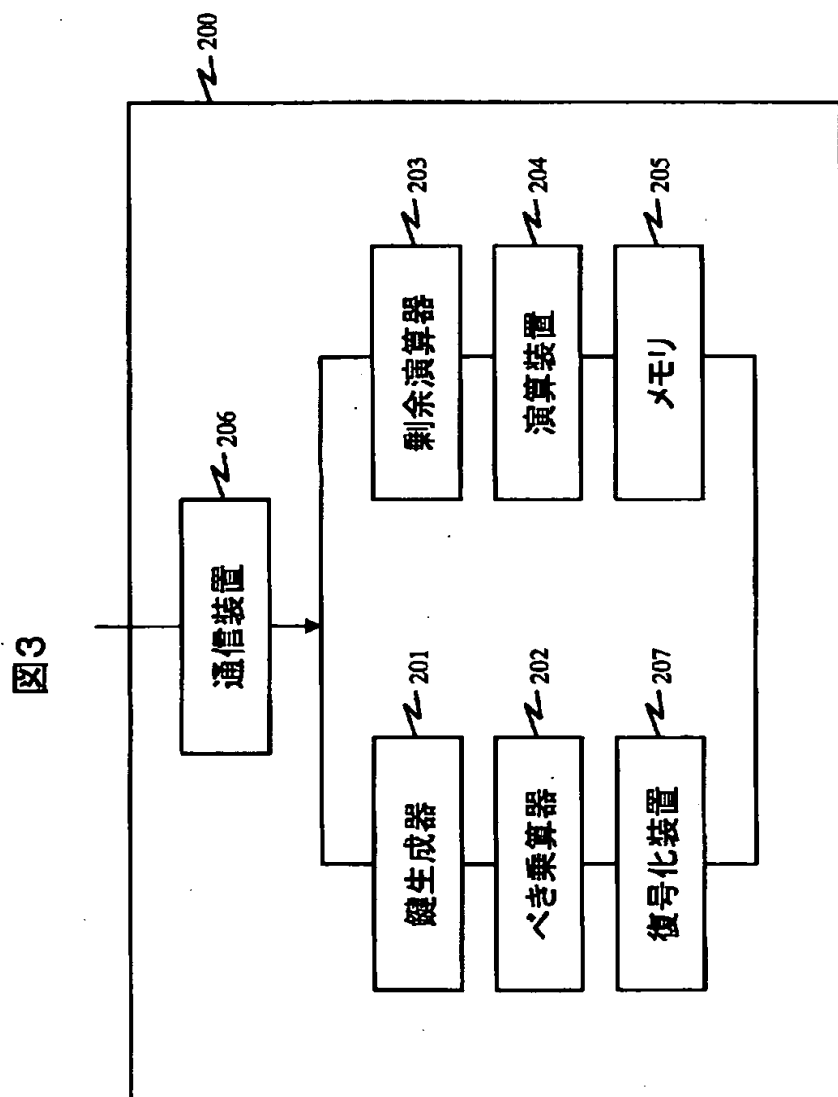
図1



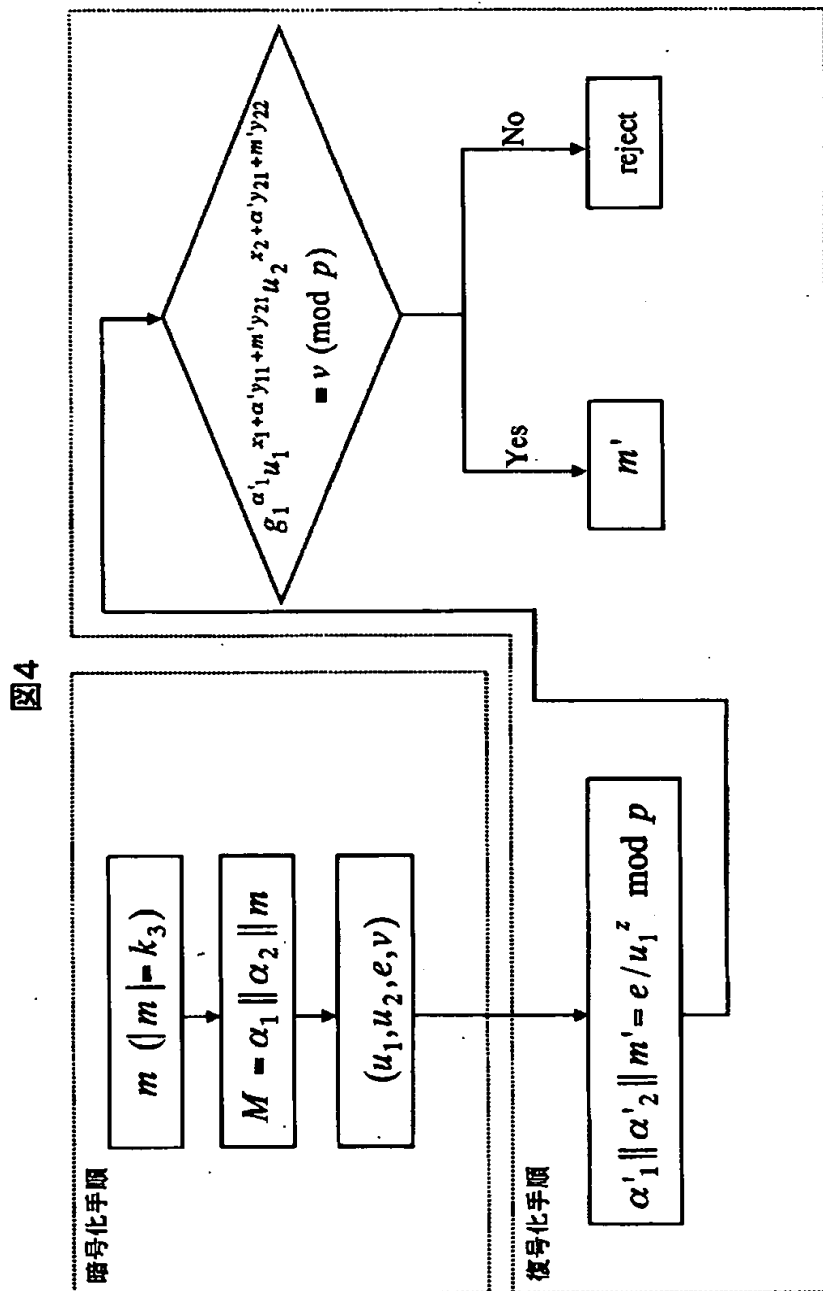
【図2】



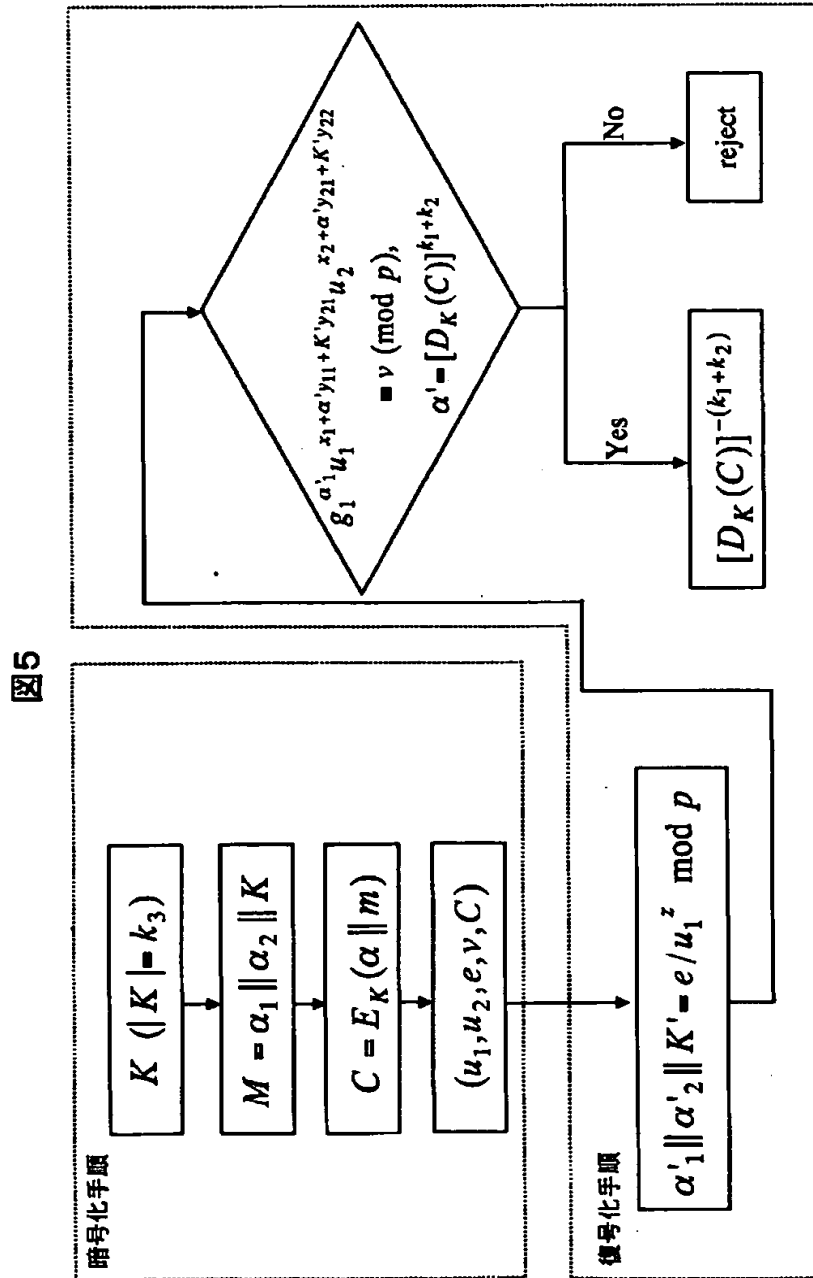
【図3】



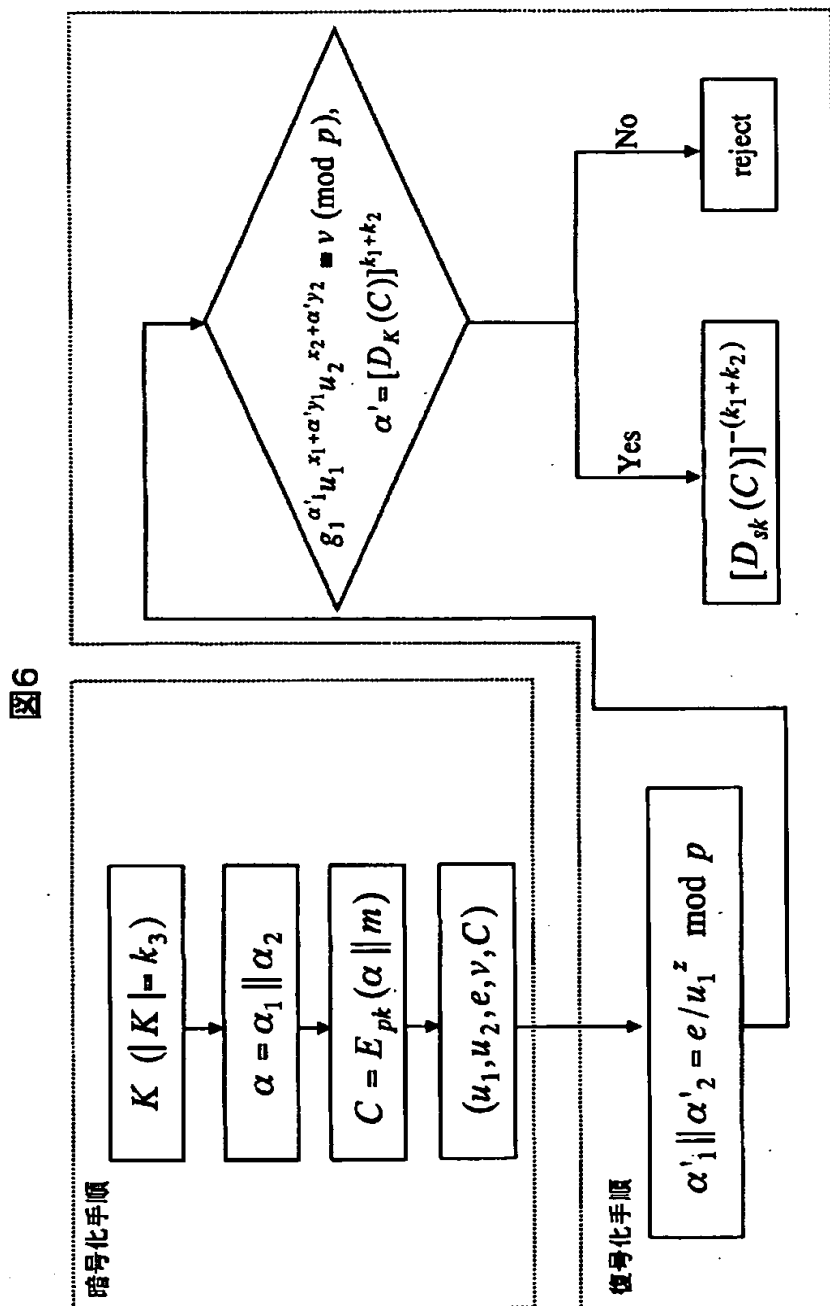
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】

標準モデル上で安全性の証明が可能であり、かつ、効率性の高い公開鍵暗号方法を提供する。

【解決手段】

適応的選択暗号文攻撃に対しての安全性を確保するため、不正な暗号文が（シミュレートされた）復号化オラクルに入力された場合には拒否されるように、平文と乱数を組み合わせて暗号文を作成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所